Secure ACS per Windows v3.2 con autenticazione computer EAP-TLS

Sommario

Introduzione

In questo documento viene descritto come configurare Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) con Cisco Secure Access Control System (ACS) per Windows versione 3.2.

Nota: l'autenticazione del computer non è supportata con Novell Certificate Authority (CA). ACS può utilizzare EAP-TLS per supportare l'autenticazione del computer in Microsoft Windows Active Directory. Il client utente finale potrebbe limitare il protocollo per l'autenticazione utente allo stesso protocollo utilizzato per l'autenticazione del computer. Ciò significa che l'utilizzo di EAP-TLS per l'autenticazione dei computer potrebbe richiedere l'utilizzo di EAP-TLS per l'autenticazione degli utenti. Per ulteriori informazioni sull'autenticazione dei computer, fare riferimento alla sezione

Machine Authentication del manuale *utente di Cisco Secure Access Control Server 4.1*.

Nota: quando si imposta ACS per l'autenticazione dei computer tramite EAP-TLS e ACS è stato impostato per l'autenticazione dei computer, il client deve essere configurato per eseguire solo l'autenticazione dei computer. Per ulteriori informazioni, vedere Come attivare l'autenticazione basata solo sul computer per una rete basata su 802.1X in Windows Vista, Windows Server 2008 e Windows XP Service Pack 3.

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate di seguito.

- Cisco Secure ACS per Windows versione 3.2
- Servizi certificati Microsoft (installato come Autorità di certificazione radice dell'organizzazione [CA])**Nota:** per ulteriori informazioni, consultare la Guida dettagliata all'impostazione di un'Autorità di certificazione .
- Servizio DNS con Windows 2000 Server con Service Pack 3 e hotfix 323172**Nota:** se si verificano problemi con il server CA, installare l'hotfix 323172 . Il client Windows 2000 SP3 richiede l'hotfix 313664 per abilitare l'autenticazione IEEE 802.1x.
- Cisco Aironet serie 1200 Wireless Access Point 12.01T
- IBM ThinkPad T30 con Windows XP Professional e Service Pack 1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nozioni di base

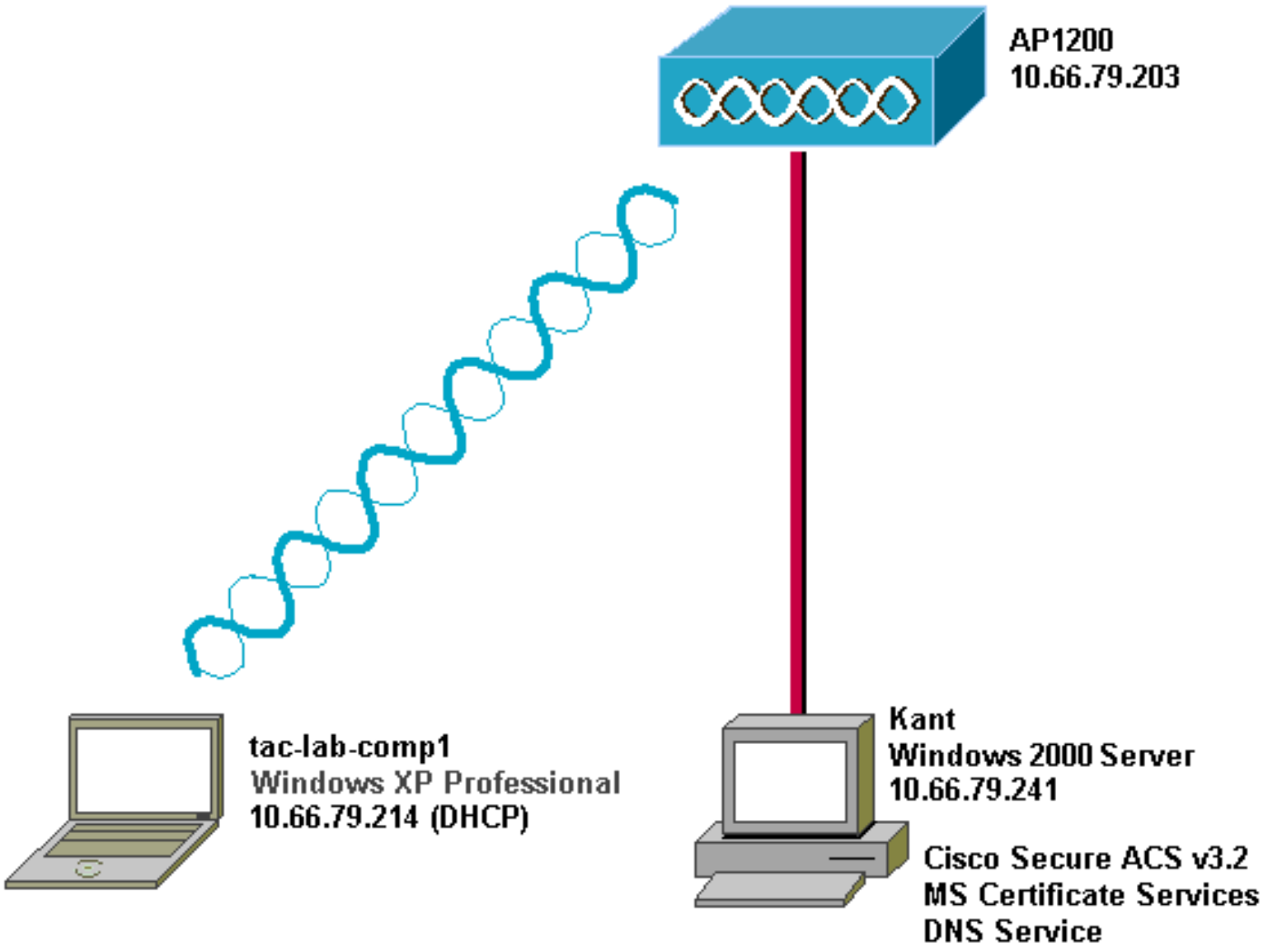
Sia EAP-TLS che PEAP (Protected Extensible Authentication Protocol) generano e utilizzano un tunnel TLS/Secure Socket Layer (SSL). EAP-TLS utilizza l'autenticazione reciproca in cui sia il server ACS (Authentication, Authorization, and Accounting [AAA]) che i client dispongono di certificati e si scambiano le rispettive identità. PEAP, tuttavia, utilizza solo l'autenticazione sul lato server; solo il server dispone di un certificato e ne dimostra l'identità al client.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



Configurazione di Cisco Secure ACS per Windows v3.2

Per configurare ACS 3.2, procedere come segue.

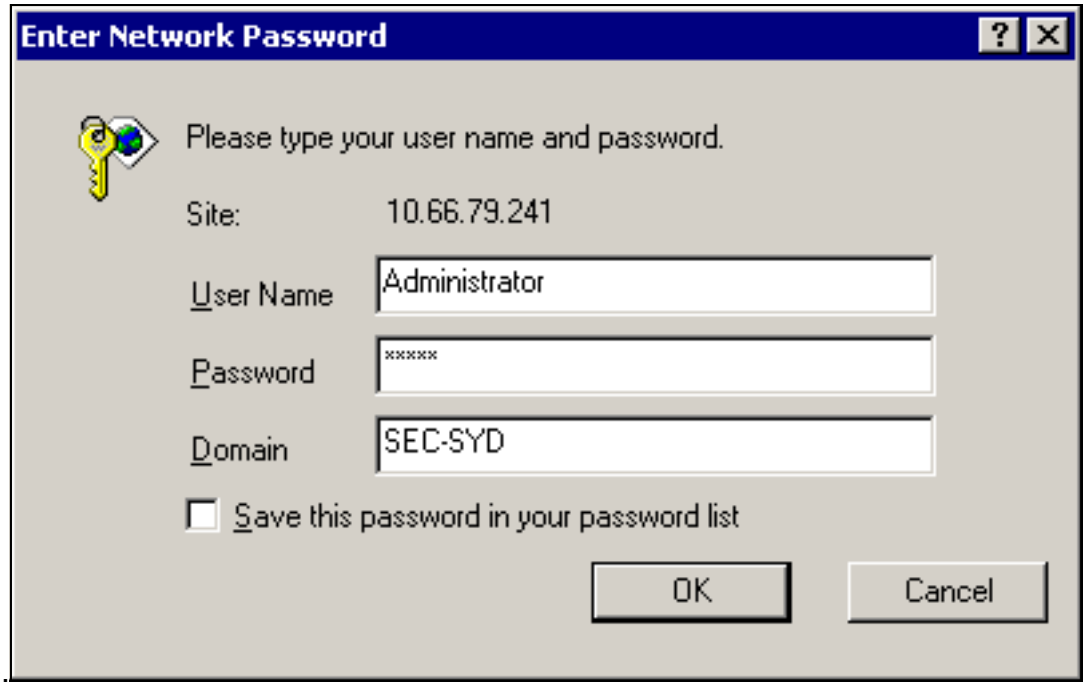
1. Ottenere un certificato per il server ACS.
2. Configurare ACS per l'utilizzo di un certificato di archiviazione.
3. Specificare le autorità di certificazione aggiuntive da considerare attendibili per ACS.
4. Riavviare il servizio e configurare le impostazioni PEAP su ACS.
5. Specificare e configurare il punto di accesso come client AAA.
6. Configurare i database utente esterni.
7. Riavviare il servizio.

Ottenere un certificato per il server ACS

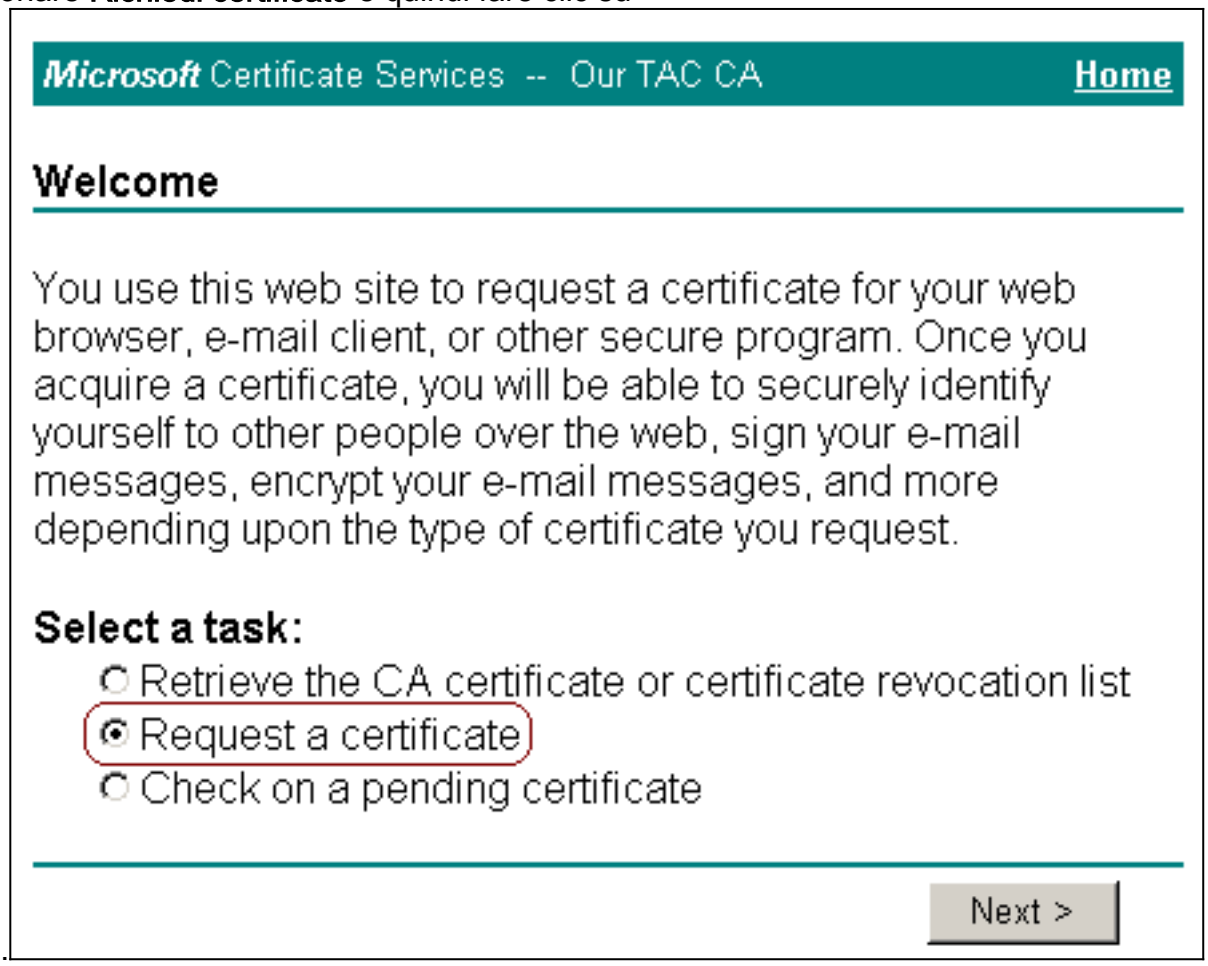
Per ottenere un certificato, eseguire la procedura seguente.

1. Sul server ACS, aprire un browser Web e immettere **http://*CA-ip-address*/certsrv** per accedere al server CA.
2. Accedere al dominio come

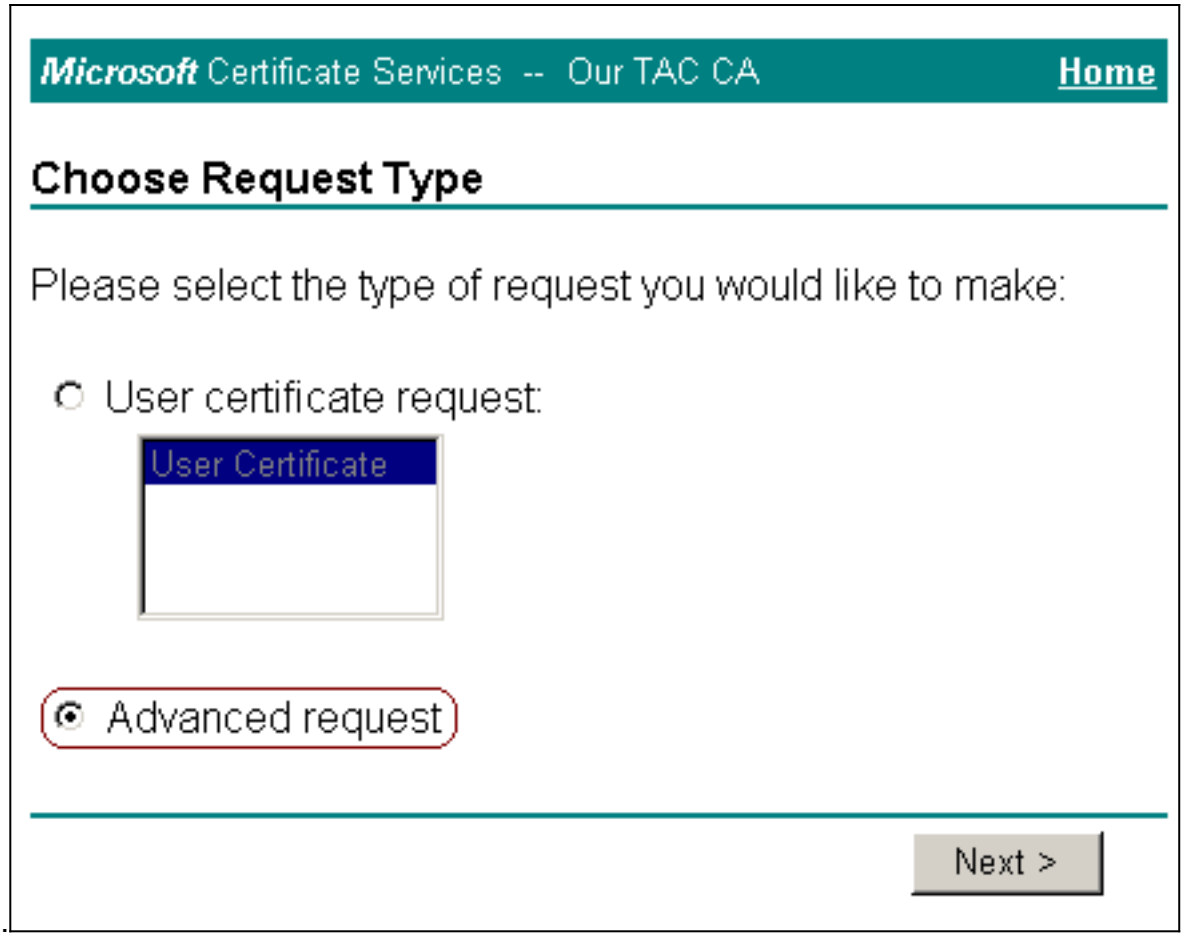
amministratore.



3. Selezionare **Richiedi certificato** e quindi fare clic su **Avanti**.

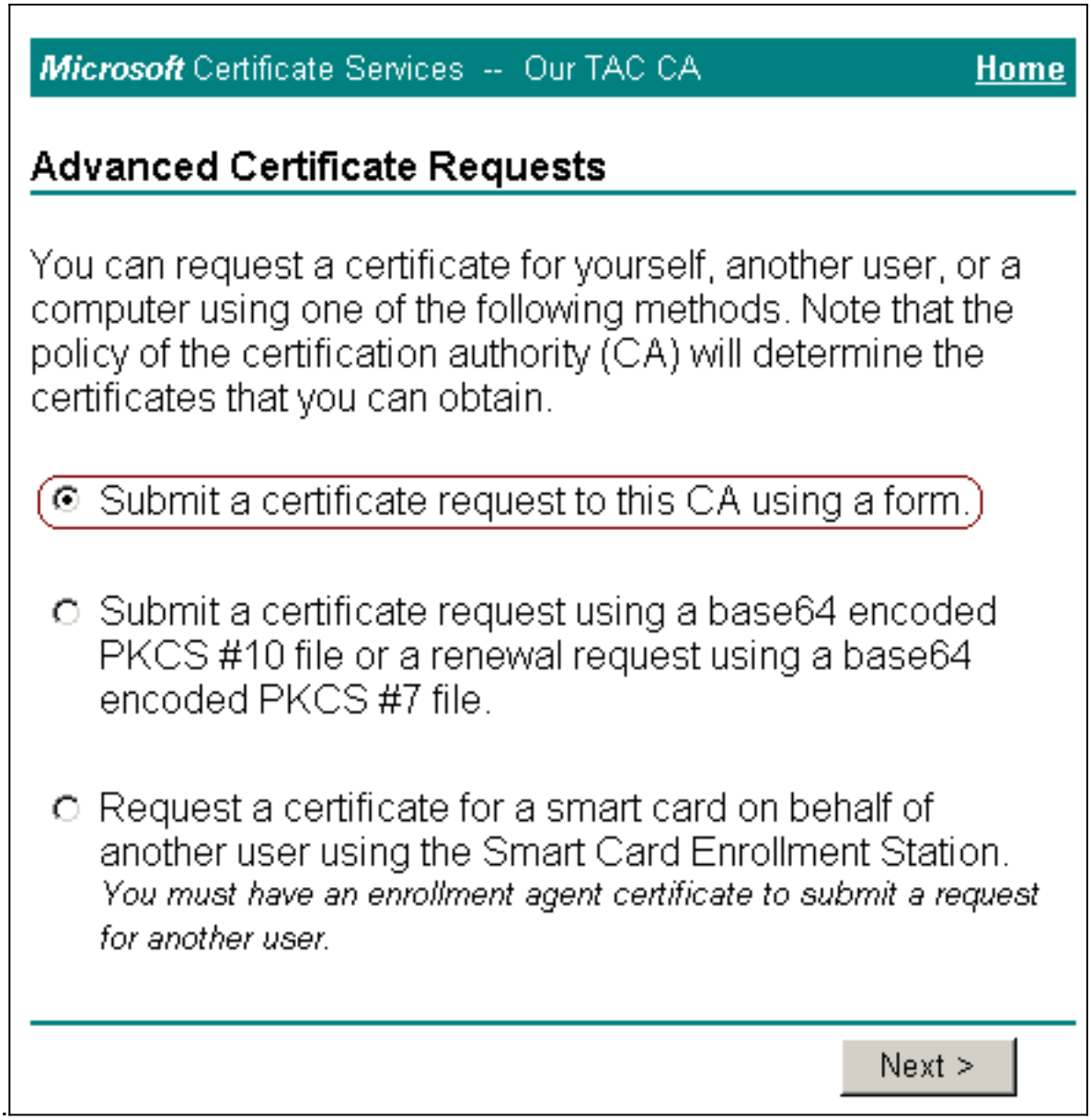


4. Selezionare **Richiesta avanzata**, quindi fare clic su



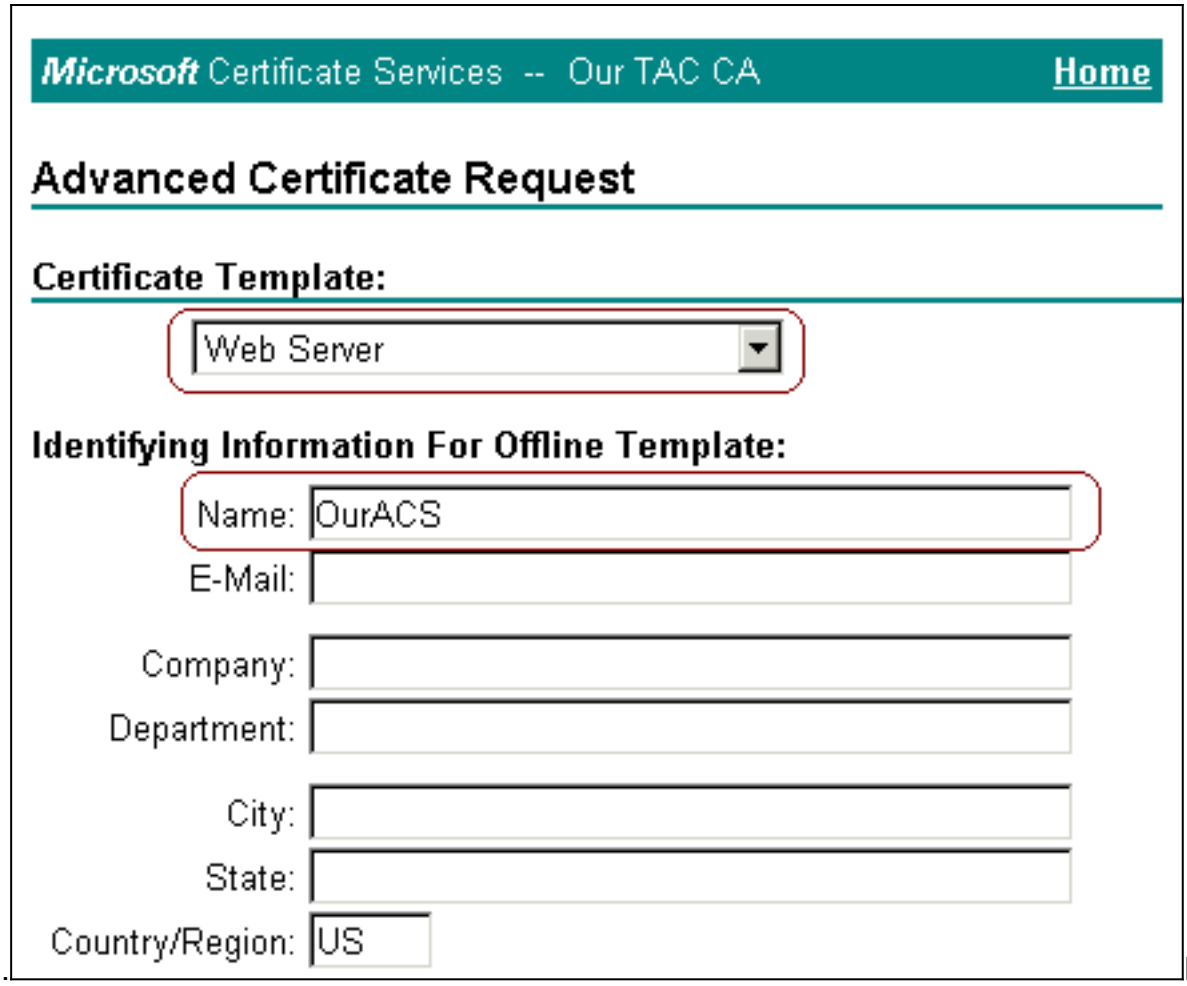
Avanti.

5. Selezionare **Invia una richiesta di certificato a questa CA utilizzando un modulo**, quindi fare clic su

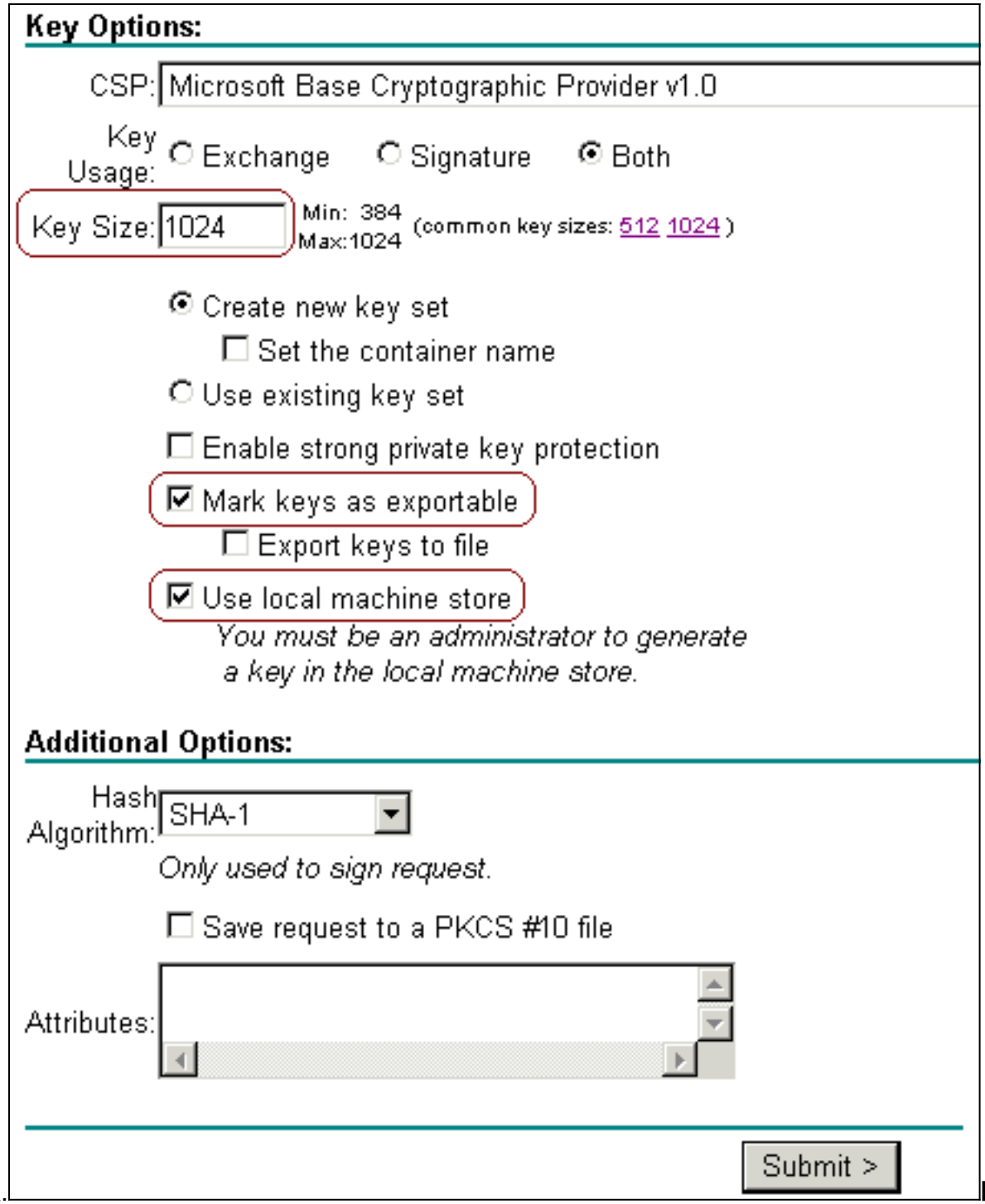


Avanti.

6. Configurare le opzioni del certificato:Selezionare **Server Web** come modello di certificato e immettere il nome del server

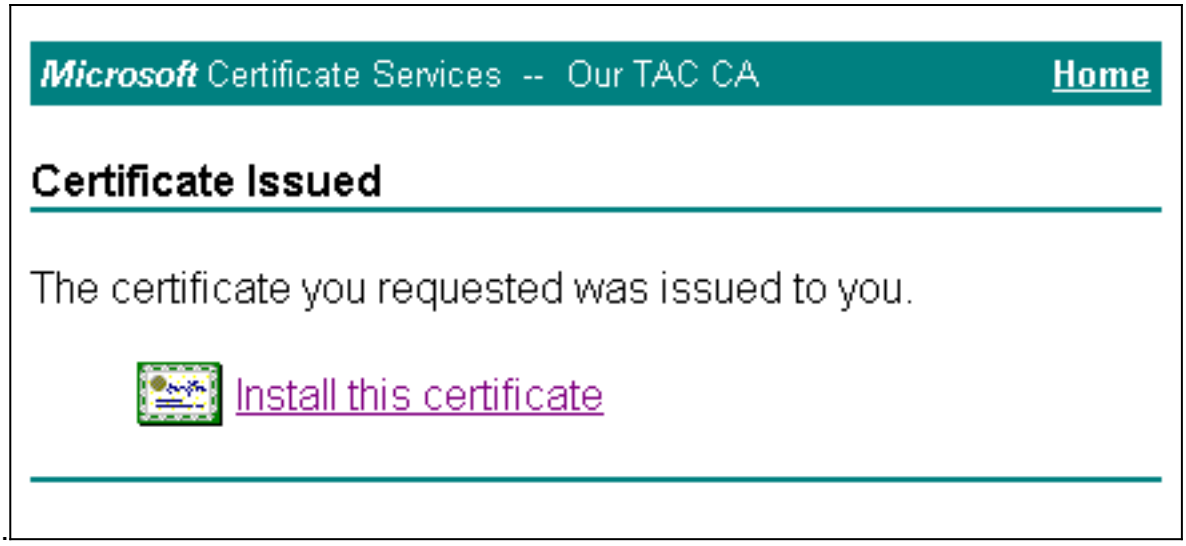


ACS.Immettere **1024** nel campo Dimensione chiave e selezionare le caselle di controllo **Contrassegna le chiavi come esportabili** e **Usa archivio locale**.Configurare altre opzioni in base alle esigenze e quindi fare clic su



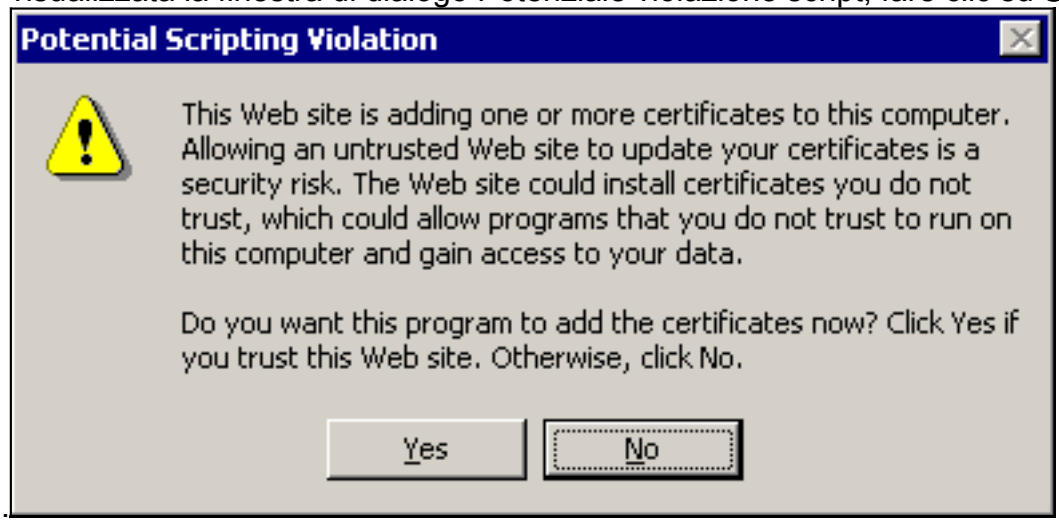
Invia. **Nota**: se viene visualizzata la finestra di dialogo Potenziale violazione script, fare clic su **Sì** per continuare.

7. Fare clic su **Installa il**

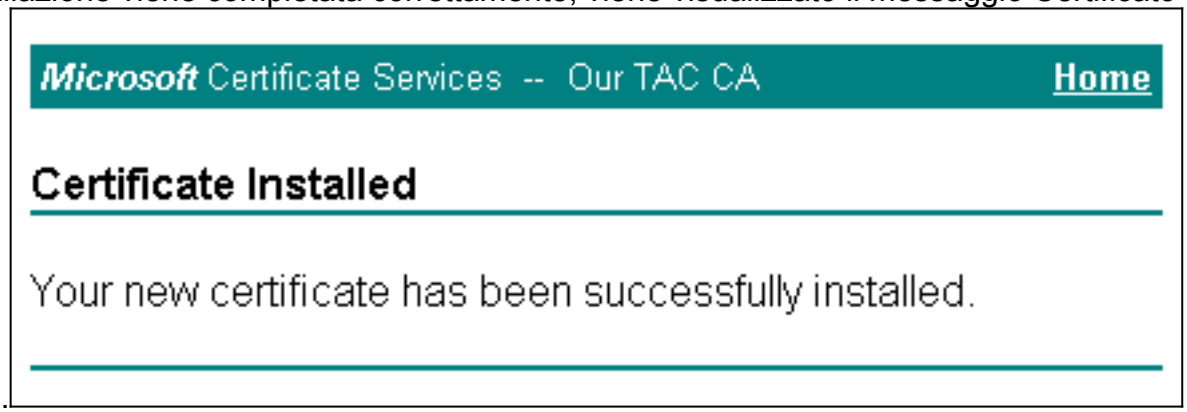


certificato.

Nota: se viene visualizzata la finestra di dialogo Potenziale violazione script, fare clic su **Sì** per continuare.



8. Se l'installazione viene completata correttamente, viene visualizzato il messaggio Certificato installato.



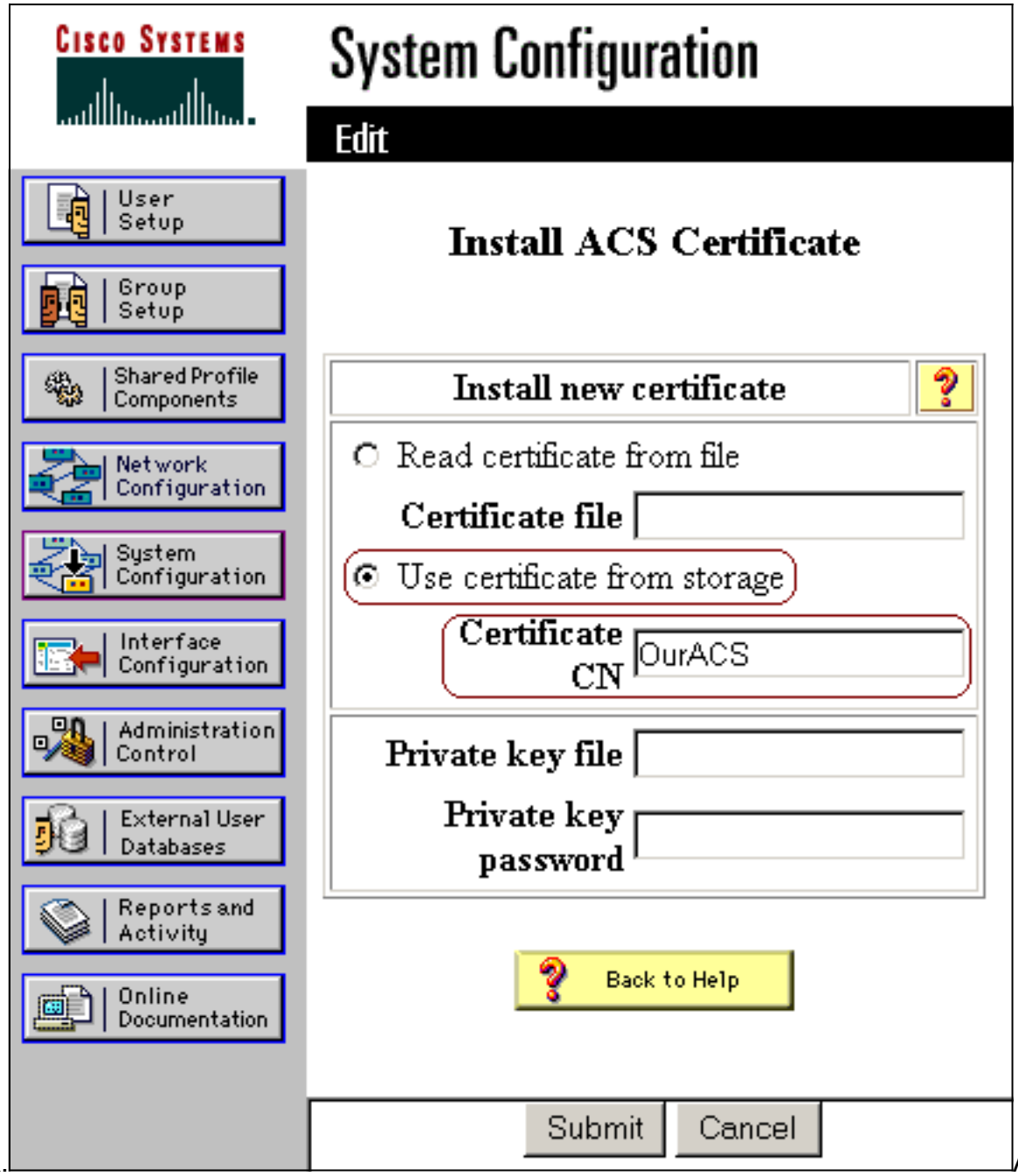
Configurazione di ACS per l'utilizzo di un certificato dall'archivio

Completare questa procedura per configurare ACS in modo che utilizzi il certificato in archiviazione.

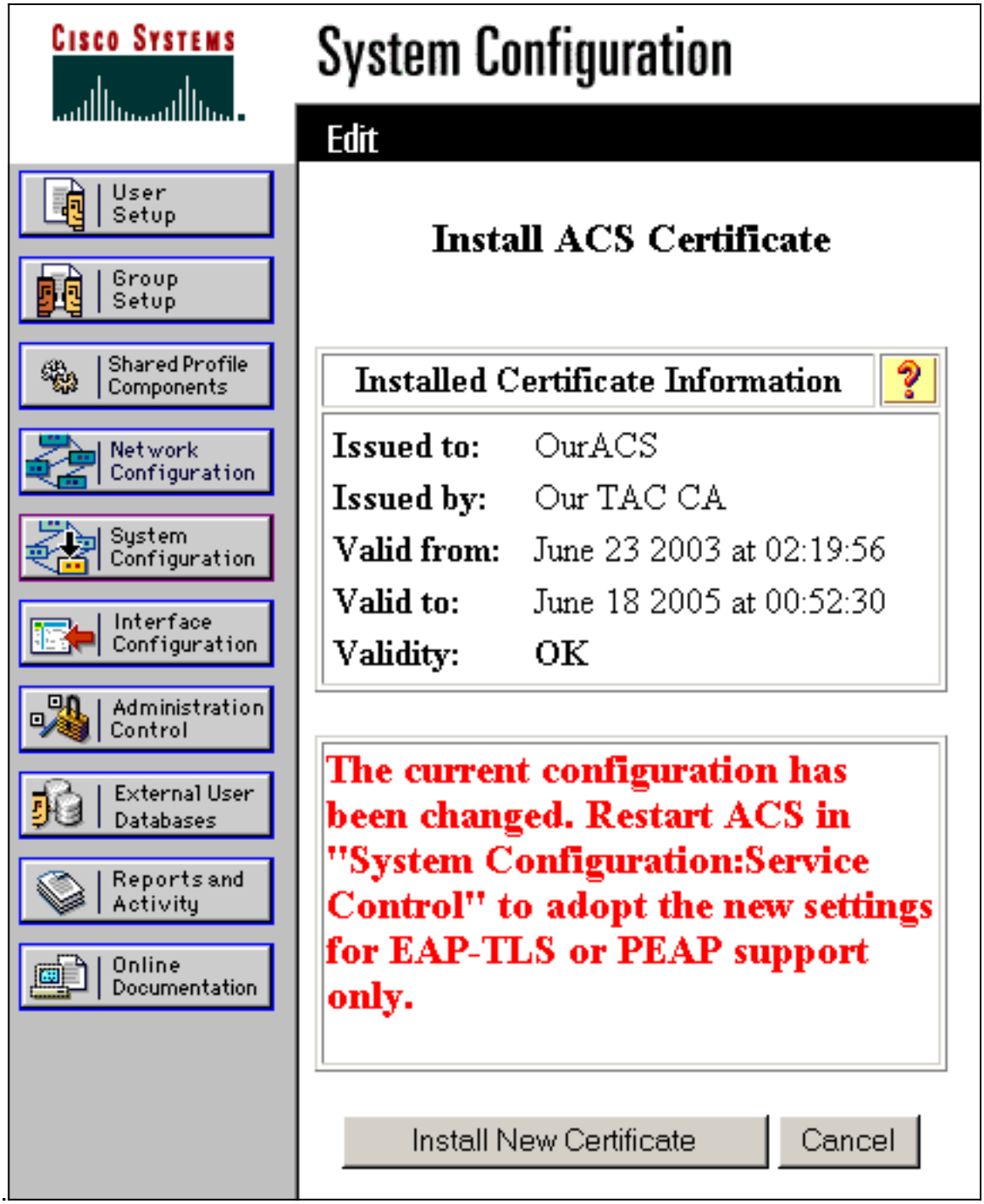
1. Aprire un browser Web e immettere **http://*ACS-ip-address*:2002/**a per accedere al server ACS.
2. Fare clic su **Configurazione di sistema**, quindi su **Configurazione certificato ACS**.
3. Fare clic su **Installa certificato ACS**.
4. Fare clic sul pulsante di opzione **Usa certificato da archiviazione**.
5. Nel campo Certificato CN, immettere il nome del certificato assegnato al passaggio 5a di

Ottenere un certificato dalla sezione del server ACS di questo documento.

6. Fare clic su



Invia. Al termine della configurazione, viene visualizzato un messaggio di conferma che indica che la configurazione del server ACS è stata modificata.**Nota:** al momento non è necessario riavviare

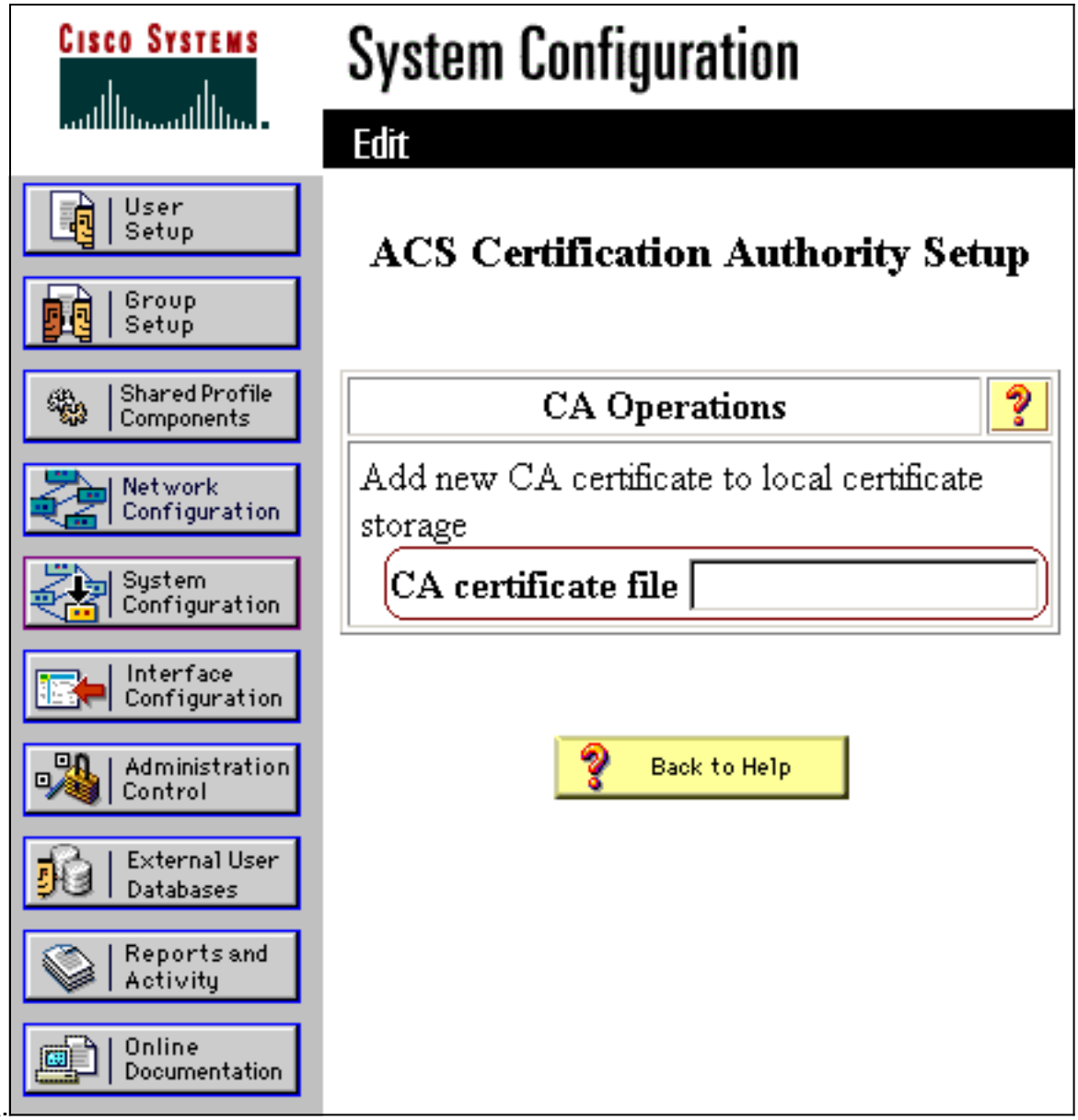


l'ACS.

Specificare Autorità di certificazione aggiuntive da considerare attendibili per ACS

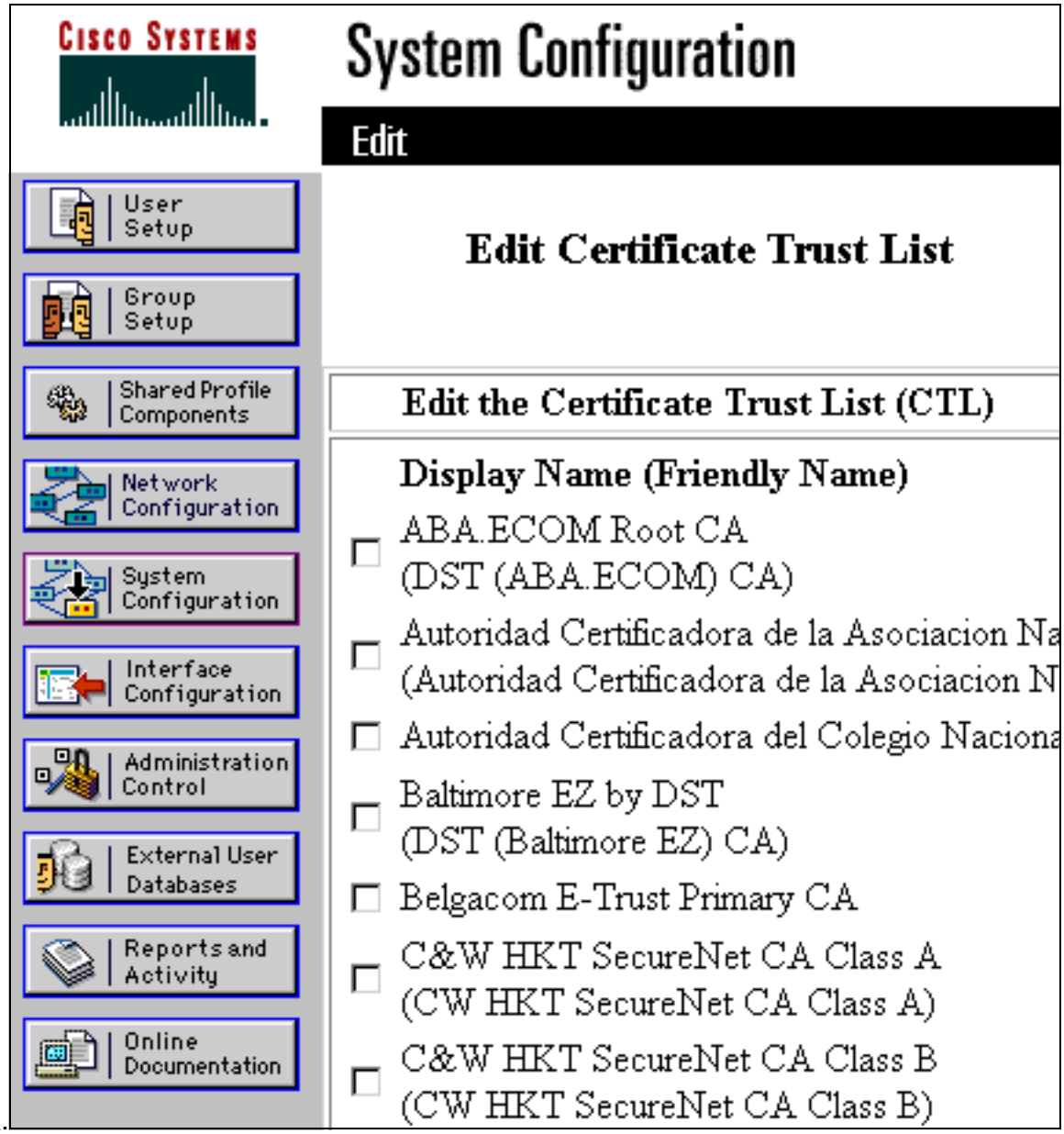
L'ACS considera automaticamente attendibile la CA che ha emesso il proprio certificato. Se i certificati client vengono emessi da CA aggiuntive, completare i seguenti passaggi:

1. Fare clic su **Configurazione di sistema**, quindi su **Configurazione certificato ACS**.
2. Fare clic su **Installazione Autorità di certificazione ACS** per aggiungere le CA all'elenco dei certificati attendibili.
3. Nel campo relativo al file del certificato CA, immettere il percorso del certificato e fare clic su



Invia.

4. Fare clic su **Modifica elenco scopi consentiti ai certificati**.
5. Selezionare tutte le CA che ACS deve considerare attendibili e deselezionare tutte le CA che ACS non deve considerare attendibili.
6. Fare clic su



Invia.

Riavviare il servizio e configurare le impostazioni EAP-TLS su ACS

Completare questa procedura per riavviare il servizio e configurare le impostazioni EAP-TLS:

1. Fare clic su **Configurazione di sistema** e quindi su **Controllo servizio**.
2. Per riavviare il servizio, fare clic su **Restart** (Riavvia).
3. Per configurare le impostazioni EAP-TLS, fare clic su **Configurazione di sistema**, quindi su **Configurazione autenticazione globale**.
4. Selezionare **Consenti EAP-TLS**, quindi controllare uno o più confronti tra certificati.
5. Fare clic su